Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 4: Evaluating Personnel Security Information

Introduction

Objective

The Minimum Standards require your program to ensure access to relevant personnel security information in order to effectively combat the insider threat. In this lesson, you will review strategies for collecting personnel security information and see how information drawn from multiple sources can be beneficial in identifying potential insider threats.

Collecting Information

Information Sources

Ensuring that personnel security information is accessible to stakeholders in a timely manner first requires organizational components to share information. In doing this, you need to gather information from a variety of sources that includes, but is not limited to: Counterintelligence, security, human resources, and Information assurance.

Information collected from multiple sources assists your program in creating a comprehensive picture of a potential insider threat.

Counterintelligence

Information from counterintelligence includes, but may not be limited to counterintelligence files, foreign travel, and foreign contacts.

Security

Information from security should include, but may not be limited to: a variety of records and reports, security clearance adjudications, as well as information security clearance adjudications. Take a moment to review this list of possible security information sources.

- Facility access records
- Financial disclosure filings
- Security incident files
- Serious incident reports
- Inspector General reports
- Security clearance adjudications
- Polygraph results
- Foreign travel
- Foreign contacts

Human Resources

Information from human resources may include personnel files, payroll information, and other files. Take a moment to review this list of possible human resources information sources.

- Personnel files
- Payroll and voucher files
- Outside work/activities requests
- Disciplinary files

Information Assurance

Possible information from information assurance, or IA, might include different types of network access information and logs. Take a moment to review this list of possible IA information sources.

- Personnel usernames and aliases
- Levels of network access
- Unauthorized use of removable media
- Print logs
- IT audit logs

Evaluating Information

Collecting information from multiple sources will assist your program in creating a comprehensive picture of an individual. Evaluated as a whole, this picture may help confirm a potential insider threat. For example, a print log might show that an individual has been printing an unusually large amount of documents. On its own, this might not raise any flags – there could be a reasonable explanation for the printing. However, combining it with additional pieces of information might change how you see the situation.

Example

Notice the information from the employee's disciplinary file: Her performance has dropped and it's noted that she is hostile toward coworkers and managers.

from Disciplinary File

…the employee's performance has dropped off significantly…

…often hostile towards coworkers and managers…

Also note times listed in the Facility Access Records. This is outside of regular duty hours and, as it turns out, some of these times coincide with the increased print activity previously noted.

from Facility Access Records

Employee Access Time Log

Wednesday	11:34PM
Saturday	08:15PM
Sunday	04:42PM

Viewed together, this information should raise some concerns.

Review Activity

An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened.

Select the files you may want to review concerning the potential insider threat.

- ☐ IT audit logs
- ☐ Levels of network access
- ☐ Personnel files
- ☐ Security incident files

Answer Key

Review Activity

An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened.

Select the files you may want to review concerning the potential insider threat.

- ☑ IT audit logs
- ☑ Levels of network access
- ☑ Personnel files
- ☑ Security incident files

In order to build a comprehensive picture of the individual, you should review all of these sources of information.